UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IRENE CHABAK, *individually and on behalf of all others similarly situated*, Plaintiff, v. SOMNIA, INC., Defendant.	Case No. 7:22-cv-9341 **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff Irene Chabak, individually and on behalf of all others similarly situated, brings this class action lawsuit against SOMNIA, INC. ("Somnia" or "Defendant") to obtain damages, restitution and injunctive relief for the Class, as defined herein. Plaintiff sets forth the following allegations upon information and good faith belief, except as to her own actions, the investigation of her counsel and certain facts that are a matter of public record.

NATURE OF THE ACTION

1. Defendant Somnia is a New York-based anesthesia practice management company serving medical facilities nationwide through numerous anesthesia provider practices (the "Anesthesia Providers") which it manages.

2. On or about July 11, 2022 or July 15, 2022, Somnia lost control of the highly sensitive private and medical information of the patients' of its Anesthesia Providers as a result of a data breach perpetrated by an unauthorized party which gained access to Defendant's computer system (the "Data Breach").[1]

[1] *See* Notice of Security Incident provided by Anesthesia Associates of El Paso PA, one of Defendant's Anesthesia Providers (the "Notice"), attached as **Exhibit A** hereto; *see also* https://elpasoheraldpost.com/notice-of-data-security-incident-anesthesia-associates-of-el-paso-pa/ (last accessed Oct. 25, 2022).

3. Somnia has ***not*** been forthcoming about the Data Breach, which affected almost 400,000 individuals and ***at least*** 18 anesthesia provider practices managed by Defendant:

- Anesthesia Associates of El Paso PA: 43,168 individuals impacted
- Upstate Anesthesia Services PC: 9,065 individuals impacted
- Resource Anesthesiology Associates PC: 37,697 individuals impacted
- Resource Anesthesiology Associates of IL PC: 18,321 individuals impacted
- Resource Anesthesiology Associates of CA A Medical Corporation: 16,001 individuals impacted
- Providence WA Anesthesia Services PC: 98,643 individuals impacted
- Palm Springs Anesthesia Services PC: 58,513 individuals impacted
- Lynbrook Anesthesia Services PC: 3,800 individuals impacted
- Hazleton Anesthesia Services PC: 13,607 individuals impacted
- Fredericksburg Anesthesia Services LLC: 7,069 individuals impacted
- Bronx Anesthesia Services PC: 17,802 individuals impacted
- Anesthesia Services of San Joaquin PC: 44,015 individuals impacted
- Anesthesia Associates of Maryland PC: 12,403 individuals impacted
- Grayling Anesthesia Associates PC: 15,378 individuals impacted
- Saddlebrook Anesthesia Services PC: 8,861 individuals impacted
- Mid-Westchester Anesthesia Services PC: 707 individuals impacted
- Resource Anesthesiology Associates of MO LLC: unknown number of individuals impacted
- Resource Anesthesiology Associates of MI PC: unknown number of individuals impacted.

4. While all of these Anesthesia Providers have submitted separate reports of the Data Breach to federal and/or state authorities,[2] upon investigation, information and good faith

[2] *See* The U.S. Department of Health (HHS) Office for Civil Rights (OCR) Data Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (fourteen of Defendant's affected practices filed notices of the Data Breach on September 23, 2022, listing affected victims as separate groups ranging from 3,800 (Lynbrook Anesthesia Services) to 98,643 individuals (Providence WA Anesthesia Services).

Resource Anesthesiology Associates of MO LLC and Resource Anesthesiology Associates of MI PC have not filed with the HHS but, along with eight other affected practices, filed notices of the Data Breach with Attorney General of Montana on October 24, 2022. *See* Montana DOJ Data Breach Incidents Database, https://dojmt.gov/consumer/databreach/ (last accessed Oct. 25, 2022).

belief, Somnia itself has thus far made only a limited disclosure of the data breach involving only 1,326 patients in NY[3] – despite the fact that 18 of its affiliates report that on July 11, 2022 or July 15, 2022 a "data security incident impacting its Management Company" occurred "that may have resulted in the compromise of protected health information for the Provider's patients."[4]

5. It appears that Somnia is trying to completely avoid any and all responsibility for the Data Breach, and is using its local practices to obscure the identity of the responsible entity as well as to downplay the severity of the Data Breach, which compromised Private Information of more than 400,000 victims. [5]

6. On October 24, 2022, or more than three months after the Data Breach occurred, ten of Defendant's Anesthesia Providers disclosed the Data Breach to the Attorney General of Montana.[6] Montana disclosures attach identical data breach notification letters for each of Defendant's affiliate practices ("Notices").[7]

7. These Notices are not only extremely vague but also legally inadequate. First, they obscure that fact that Somnia is the responsible party which exposed (or, at least, left vulnerable)

---

[3] *See* HHS OCR Data Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Somnia waited until October 24, 2022 to file a report of the data breach for "Somnia, Inc." with the federal authorities) (last accessed Oct. 31, 2022).

[4] *See* **Exhibit A**; *see also* Notice Of Data Security Incident issued by Anesthesia Associates of El Paso PA, https://elpasoheraldpost.com/notice-of-data-security-incident-anesthesia-associates-of-el-paso-pa/l; Notice Of Data Security Incident issued by Grayling Anesthesia Associates PC, https://crawfordcountynow.com/local/legal-notice-from-grayling-anesthesia-associates-pc/; https://dojmt.gov/consumer/databreach/.

[5] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[6] *See* https://dojmt.gov/consumer/databreach/ (last accessed Oct. 27, 2022).

[7] *Compare* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf, *with* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-649.pdf.

patients' highly sensitive Private Information, stating instead that provider's "*management company* identified suspicious activity on its systems" which resulted in loss of access to some of Somnia's systems, and that patients' "protected health information *may have been affected*" (emphasis added).[8]

8. Second, the Notices fail to disclose exactly what information has been affected or how many patients had their Private Information compromised, vaguely stating that impacted information stored in Defendant's systems "may include" "some combination" of patient names, Social Security numbers, date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis."[9]

9. Defendant's Anesthesia Providers offer conflicting information regarding when the Data Breach occurred, how long it lasted, and how quickly Defendant reacted to the Data Breach. Montana DOJ disclosures state that the Data Breach and "suspicious activity" on Defendant's computers took place on July 11, 2022, and that Somnia "immediately implemented its incident response protocols, [and] disconnected all systems."[10] However, disclosures to the

---

[8] *See id.*; *see also* Legal Notice from Grayling Anesthesia Associates PC, https://crawfordcountynow.com/local/legal-notice-from-grayling-anesthesia-associates-pc/ ("a data security incident impacting its *Management Company* […] *may have resulted* in the compromise of protected health information for the Provider's patients" (last accessed Oct. 25, 2022).

[9] Each Notice consists of two template letters which are identical save for patients' impacted information. One letter states that compromised information may include a patient's name, "date of birth, driver's license number, financial account information, health insurance policy number, Medical record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info." The second template letter adds patients' Social Security Number to this list. *See* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf; https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-649.pdf.

[10] *See* https://dojmt.gov/consumer/databreach/; *see also* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf.

HHS OCR stated that the Data Breach occurred on July 15, 2022.[11] It is not clear whether Defendant does not know when the Data Breach took place, or whether it is trying to obscure the severity of impact on its systems and/or the amount of time it took Defendant to restore control over its networks and patients' sensitive Private Information.

10. It is not even possible to determine from Somnia's template Notices how many months of credit monitoring services are being offered to all of the affected victims.[12]

11. Finally, while the intrusion of Defendant's network occurred in early July 2022, Somnia inexplicably waited ***another two months*** after that—until September 21, 2022 at the earliest—to begin to issue notice to affected persons and to notify the authorities and even then—as noted herein—obliquely did so through its various anesthesia provider practices.

12. After a data breach, most companies at least try to make it appear as if they are taking appropriate steps to secure their customers' Private Information. Somnia is not even pretending it is doing what is necessary and appropriate to inform and to protect 406,376 affected individuals whose personal and highly sensitive data has been compromised.

13. As detailed above, the Private Information exposed in the Data Breach included, among other things: patient names, addresses, health insurance policy numbers, Social Security numbers, financial account information, date of birth, driver's license numbers, and various highly sensitive medical information.[13]

---

[11] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf; *see also* https://elpasoheraldpost.com/notice-of-data-security-incident-anesthesia-associates-of-el-paso-pa/; https://crawfordcountynow.com/local/legal-notice-from-grayling-anesthesia-associates-pc/.

[12] *See* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf (template provides a choice of 12 or 24 months of credit monitoring).

[13] *See* **Exhibit A**; https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf; https://elpasoheraldpost.com/notice-of-data-security-incident-anesthesia-associates-of-el-paso-pa/.

14. Despite the prevalence of ransomware and other data security attacks in recent years, the Data Breach was a direct result of Defendant's abject failure to implement and to maintain adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and the Class Members' Private Information.

15. The nature of the cyberattacks and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendant and thus Defendant was on—at least, constructive—notice that failing to take steps necessary to secure the Private Information from those risks left the information in an extremely dangerous and needlessly vulnerable condition.

16. Defendant disregarded the rights of Plaintiff and the Class Members by, *inter alia*, (i) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Members' PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach, and (iv) failing to provide Plaintiff and the Class Members with a prompt, complete and accurate notice of the Data Breach.

17. Upon information and good faith belief, had Somnia properly maintained and monitored its property, it could have prevented and/or discovered the intrusion sooner.

18. Plaintiff's and the putative Class Members' identities are now at risk because of Defendant's conduct since the Private Information that Defendant obtained and maintained is now in the hands of data thieves.

19. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including perpetrating medical and financial identity theft.

20. Medical theft occurs when someone steals or uses patients' Private Information

(*e.g.*, name, Social Security number or Medicare number), to see a doctor, obtain prescription drugs, buy medical devices, submit fraudulent claims to Medicare or an insurance carrier, and/or obtain other medical care.

21. Moreover, if a medical identity thief's information is combined with an affected patient, it could seriously impair the affected individual's medical care and/or the health insurance benefits they are able to obtain. Such identity theft can also negatively impact credit scores and wastes taxpayer dollars.[14]

22. Identity thieves use stolen personal information such as Social Security numbers for a variety of financial crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

23. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud, financial identity theft, and medical identity theft.

24. Plaintiff and Class Members must now and in the future closely monitor ***all*** of their financial and health information and accounts to guard against fraud and identity theft. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports or other protective measures to detect and to deter such identity theft.

25. Plaintiff therefore brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their Private Information had been subject to the unauthorized access of an unknown third party and to specify the types of information accessed.

---

[14] *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Oct. 19, 2022).

26. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

27. Plaintiff is, and was at all relevant times, an individual citizen residing in El Paso County in the State of Texas.

28. Defendant Somnia Inc., also doing business as Somnia Anesthesia, is a private anesthesia practice management and perioperative medical company, incorporated and headquartered in the State of New York. Defendant Somnia provides anesthesia management and perioperative services to more than 100 surgery centers and medical offices across the U.S.

29. The principal place of business and headquarters of Defendant Somnia, located at 450 Mamaroneck Ave, Suite 201 Harrison, New York, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate Defendant's and its anesthesia provider practices' activities, including, but not limited to, major policy, financial and legal decisions.

JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) ("CAFA") as the amount in controversy exceeds $5 million, exclusive of interest and costs and, upon information and good faith belief based on Defendant's public representations, the number of affected individuals is at least 406,376, many of whom have different citizenship from Defendant.

31. This Court has personal jurisdiction over Defendant because it transacts business, contracts to supply services and has caused tortious injury by act or omission with the State of

New York. In addition, Defendant has its principal place of business located at 450 Mamaroneck Ave, Suite 201, Harrison, New York, and the computer systems implicated in this Data Breach are likely based in this District. By and through its business operations in this judicial district, Defendant intentionally avails itself of the markets within this judicial district so as to render the exercise of jurisdiction by this Court just and proper.

32. Venue is proper pursuant to 28 U.S.C. § 1391(a)(1) because Defendant is resident in this District, maintains the Private Information at issue in this lawsuit in this District and has caused harm to Class Members residing in this District. Venue is therefore appropriate because a substantial portion of the events giving rise to this action occurred in this District.

STATEMENT OF FACTS

A. The Data Breach.

33. On or about July 11, 2022 or July 15, 2022, Somnia lost control over Plaintiff's and the putative Class Members' Private Information when cybercriminals accessed patients' files on Defendant's computer systems.

34. Even though the intrusion occurred on or about July 11, 2022 or July 15, 2022, it was not until two months later that Somnia's various anesthesia provider practices began to notify the authorities and some of them began issuing notice to the victims.

35. According to the Notices of Security Incident, Private Information exposed in the Data Breach included, among other things: patient names, addresses, driver's license numbers, health insurance information, Medicaid or Medicare ID, Social Security numbers and various sensitive personal "health information."[15]

[15] *See* **Exhibit A;** *see also* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf.

36. The information provided in the Notices and on the U.S. Department of Health and Human Services Office for Civil Rights Data Breach Portal regarding the Data Breach is noticeably scant.[16]

37. Defendant's Notices do not indicate what entity attacked it or whether its system was encrypted or otherwise secured in any fashion prior to the attack.[17]

38. Defendant declines to name a single specific thing that it did other than wait nearly two months to begin to provide notice.

39. Defendant's Notices attempt to minimize the extent of harm to Plaintiff and Class Members by stating that "[i]nformation stored in the Management Company's system *could include some combination* of patient names, addresses, health insurance policy number, Social Security numbers, payment information, and health information such as treatment and diagnosis" (emphasis added).[18]

40. Defendant does not discuss why it took more than two months from the date of the Data Breach to begin to issue notice.[19]

41. The reason that Somnia is being less than forthcoming is because the Data Breach was a direct result of its failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information.

---

16 *Id.*; *see also* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

17 *See* **Exhibit A**; *see also* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf.

18 *Id.*

19 Somnia is being purposively evasive about the information conveyed because it is more concerned with trying to limit its exposure than it is providing complete and accurate information to more than 400 thousand persons affected by this Data Breach so that they can take preventative and/or precautionary measures.

B. Defendant's Responsibility to Safeguard Information.

42. Defendant provides anesthesia management and perioperative services to more than 100 medical facilities across the U.S.[20]

43. In the course of doing business, Somnia collects very sensitive information about its patients including their Private Information.

44. This sensitive information is provided by patients to Defendant for healthcare related services.

45. Defendant is required by law to maintain the privacy and security of patients' protected health information, and to develop and distribute a notice that provides a clear, user friendly explanation of individuals rights with respect to their personal health information and Defendant's privacy practices.[21]

46. In stark contrast to model notices provided by the HHS, Defendant's Legal page has only general language regarding protecting patients' PHI:

> Somnia, Inc. and its affiliates [] are committed to fulfilling their obligations under Health Insurance Portability and Accountability Act (HIPAA) and to safeguarding the protected health information (PHI) of patients. At Somnia, we are guided by our respect for the confidentiality of patient PHI, and we will not disclose this information to anyone without getting patient consent or an authorized person(s), unless we are permitted to do so by law.[22]

47. Defendant completely fails to inform its patients and customers how their PHI may be used or disclosed, legitimate uses and disclosures that do not require patient's

---

[20] *See* http://somnia.s7.devpreviewr.com/outpatient-facilities/ (last accessed Oct. 26, 2022).

[21] *See* HHS Guidance on Model Notices of Privacy Practices, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html (last accessed Oct. 26, 2022).

[22] *See* https://somniaanesthesiaservices.com/legal/ (last accessed Oct. 26, 2022).

authorization, uses and disclosures that require written consent, rights with respect to PHI, or notification in the event of an unauthorized use or disclosure.[23]

48. The only other "privacy policy" on Defendant's website is limited to "personal information" (which includes a person's "name, mailing address (including zip code), country of residence, e-mail address, telephone and facsimile numbers") collected and used by Somnia, its affiliates and agents, through its website "in order to record, support and facilitate services provided in this Internet web site."[24] Defendant also lists additional legitimate uses of such personal information, including sending information on services provided by Somnia to interested parties.

49. Defendant states it "recognizes and appreciates the importance of responsible use of Personal Information collected," "respects [a person's] legal rights regarding access to and correction and deletion of [their] Personal Information," and protects personal information collected through its website by storing it on "secure servers" with password-protected access for its personnel and contractors.[25]

50. Defendant then proceeds to disavow its legal duties and responsibilities to patients and customers who entrusted Defendant with their personal information:

> It is not possible, however, for SOMNIA, INC. to guarantee the security of information disclosed online to SOMNIA, INC. because no transmission of data over the Internet is totally secure and no database is totally secure from hackers, rogue employees, and the like. Personal information may also be released, erased, deleted or otherwise removed due to hacking, force majeure, accident,

---

[23] *See* HHS explanation of HIPAA Notice of Privacy Practices, https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html (last accessed Oct. 26, 2022).

[24] *See* Defendant's Privacy Policy, https://somniaanesthesiaservices.com/legal/privacy-policy/ (last accessed Oct. 26, 2022).

[25] *Id.*

> unscrupulous contractors or employees, or through other such factors, and Somnia, Inc. disclaims liability for any of the foregoing. You agree to assume all risk in connection with the information provided to SOMNIA, INC. or collected by SOMNIA, INC. when using this Internet web site.[26]

51. Somnia owed Plaintiffs and Class Members a duty to safeguard their Private Information. First, Somnia owed a duty to safeguard Private Information pursuant to a number of statutes, including the Health Insurance Portability and Accountability Act ("HIPAA") and the Federal Trade Commission Act ("FTC Act"), to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and Class Members from the type of conduct by Somnia alleged herein.

52. The patient information held by Defendant in its computer systems included the Private Information of Plaintiff and Class Members. Defendant voluntarily assumed custody of Plaintiff's and Class Members' PII and PHI for its own profit. Defendant was aware of its obligations, particularly with respect to patient PHI, as demonstrated by its Notice of Privacy Practices.

53. Next, Somnia owed a duty to safeguard Private Information as it was on notice that it was maintaining highly-valuable data for which it knew there was a risk that it would be targeted by cybercriminals. Defendant knew of the extensive harm that would occur if Plaintiff's and Class Members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information.

54. Unauthorized disclosure of Plaintiff's and Class Members' PHI and PII in this Data Breach was not for any legitimate purpose.

55. It is likely that the Data Breach was targeted at the Defendant due to its status as

---

[26] *Id*.

a healthcare entity that collects, creates, and maintains both PII and PHI.

56. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiff and Class Members.

57. Because of the Defendant's failure to properly safeguard Plaintiff's and Class Members' Private Information, data thieves were able to gain unauthorized access to Defendant's computer systems and were able to compromise, access, and acquire the protected Private Information of Plaintiff and Class Members.

58. Defendant had obligations created by HIPAA, the FTC, industry standards, state and common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

59. Given the sensitive nature of the Private Information, Somnia knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud if they were able to exfiltrate that data from Defendant's servers.

60. Somnia also knew that individuals whose Private Information was stored on its servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

61. Defendant's data security obligations were particularly important and should have been apparent given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

C. Prevalence of Cyber Attacks in Recent Years.

62. Data breaches, including ransomware attacks, are extremely commonplace.

63. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[27]

64. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[28]

65. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records, compared to only 306 breaches that exposed nearly 10 million sensitive records in 2020.[29]

66. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

67. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

68. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high

---

[27] *See* 2021 Data Breach Annual Report, at 6 (ITRC, Jan. 2022), available at https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last accessed Oct. 31, 2022).

[28] *Id.*

[29] *Id.*

incentive to regain access to their data quickly."[30]

69. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[31]

70. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

D. Somnia Acquires, Collects and Stores Class Members' Private Information.

71. As noted above, Somnia is an anesthesia practice management company serving more than 100 hospitals, ambulatory surgery centers, and office-based facilities nationwide.

72. In the course of providing these services, Somnia acquires, collects and stores a massive amount of Private Information.

73. By obtaining, collecting, and using Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from access and disclosure.

E. The Value of Private Information and the Effects of Unauthorized Disclosure.

74. Defendant was (or certainly should have been) well-aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

75. Simply put, Private Information is an extremely valuable commodity to identity

---

[30] FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974 (last accessed Oct. 31, 2022).

[31] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed Oct. 31, 2022).

thieves.

76. As the FTC recognizes, with PII and PHI identity thieves can commit an array of crimes including identify theft, medical, and financial fraud.

77. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites.

78. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe:

> Medical identity theft offers thieves a long-term income. If someone applies for credit in your name, chances are, you'll quickly notice — especially if you have alerts set up through an identity protection service.
>
> But it can take years for victims of medical identity theft to realize they've been targeted. Often, you won't know until you visit the doctor's office or need urgent treatment at the hospital.
>
> By then, a fraudster could have racked up thousands of dollars in fraudulent claims and hit your benefit limit.[32]

79. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

80. At all relevant times, Defendant knew or reasonably should have known of the importance of safeguarding Private Information and of the foreseeable consequences if its data security systems were breached, including, but not limited to, the significant costs that would be imposed on its healthcare provider clients and, most importantly, on their patients.

81. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and to safeguard the computer systems and data that held the stolen Private Information.

82. Defendant's unlawful conduct includes, but is not limited to, the following acts

[32] https://www.aura.com/learn/medical-identity-theft (last accessed Oct. 31, 2022).

and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor the data security systems for existing intrusions; and

d. Failing to ensure that its agents and service providers with access to Plaintiff's and Class Members' PII and PHI employed reasonable security procedures.

F. Defendant Did Not Comply with FTC Guidelines.

83. The Federal Trade Commission has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[33]

84. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses.[34]

85. The guidelines note that businesses should (i) protect the personal customer information that they keep; (ii) properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; (iii) understand their network's vulnerabilities; and (iv) implement policies to correct any security problems.

86. The guidelines also recommend that businesses (i) use an intrusion detection system to discover a breach as soon as it occurs, (ii) monitor all incoming traffic for activity

[33] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Oct. 31, 2022).

[34] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Oct. 31, 2022).

indicating someone is attempting to hack the system, (iii) watch for large amounts of data being transmitted from the system and (iv) have a response plan ready in the event of a breach.[35]

87. The FTC further recommends that companies (i) not maintain PII and/or PHI longer than is needed; (ii) limit access to sensitive data; (iii) require complex passwords to be used on networks; (iv) use industry-tested methods for security; (v) monitor for suspicious activity on the network and (vi) verify that third-party service providers have implemented reasonable security measures.

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

89. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

90. These FTC enforcement actions include actions against healthcare related providers like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

91. Defendant failed to properly implement basic data security practices.

92. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information constitutes an unfair act or practice

[35] *Id.*

prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

93. Defendant was at all times fully aware of its obligation to protect consumers' Private Information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Defendant Failed to Comply with Industry Standards.

94. Experts studying cybersecurity routinely identify companies that come into possession of large amounts of Private Information, such as Somnia, as being particularly vulnerable to cyberattacks because of the value of the information they maintain.

95. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

96. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

97. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in

reasonable cybersecurity readiness.[36]

98. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach and the resulting harm to Plaintiffs and the Class Members.

H. Defendant Failed to Comply with HIPAA

99. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

100. Covered entities (including Defendant) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

101. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

102. A Data Breach such as the one Defendant experienced is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition,

[36] *See* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; https://www.nist.gov/cyberframework/getting-started; *see also* https://www.cisecurity.org/controls (last accessed Oct. 31, 2022).

> access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

103. Data breaches where an unauthorized individual gains access to PHI are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *See* the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. *See* 45 C.F.R.164.308(a)(6).[37]

104. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards and standards of care mandated by HIPAA regulations.

I. Plaintiff and Class Members Suffered Damages

105. The ramifications of Defendant's failure to keep the Private Information secure are long lasting and severe.

106. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years as victims of data breaches are more likely to become victims of identity fraud.

107. The Private Information belonging to Plaintiff and Class Members is personal,

[37] *See also* Department of HHS Fact Sheet: Ransomware and HIPAA (July 11, 2016), available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed Oct. 31, 2022).

sensitive in nature and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

108. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[38] Such fraud may go undetected for months, or even years.

109. Identity thieves can also use Social Security numbers to obtain a driver's license or an official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. Each of these fraudulent activities is difficult to detect.

110. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as credit bureaus and banks will have the victim's records under the old number and will be able to use the old number to identify and connect the new number to the (compromised) old credit record.[39]

111. This data, as one would expect, demands a much higher price on the black market.

---

[38] Identity Theft and Your Social Security Number, Social Security Administration (2018); available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 31, 2022).

[39] *Id.*

Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[40]

112. Medical information is an especially valuable commodity that can be hijacked and used to falsify insurance claims or to fraudulently acquire government benefits such as Medicare or Medicaid.

113. That Private Information may also be sold on the black market where it can be used to create entirely new medical identities.[41]

114. Identity fraud of any kind can wreak havoc on a victim's life for years, but theft of PHI is especially damaging because criminals can destroy a victims' health insurance coverage and leave them without a safety net when they need it most.

115. Moreover, victims of medical identity theft could get bills for medical treatments never received.

116. In the digital age, bad data can cause a tangled mess that takes time to solve, but for people in need of urgent surgeries or treatment such delays can cause immense stress, not to mention seriously complicate the provision of needed medical treatments and services.

117. If a patient fails victim to medical identity theft, they also run the risk that Medicare and/or other health insurance benefits may be depleted when needed most.

118. Fraudulent treatments done under victims' names can completely change their medical information history, which could lead doctors to misdiagnose actual conditions or

---

[40] https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Oct. 31, 2022).

[41] https://www.consumerreports.org/health/medical-identity-theft-a1699327549/ (last accessed Oct. 31, 2022).

prescribe unnecessary treatments.

119. "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft," says Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance (MIFA), a group of several dozen healthcare organizations and businesses working to reduce the crime and its negative effects.[42]

120. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

121. Sensitive Private Information can sell for as much as $363 per record, according to the Infosec Institute.[43] PHI is particularly valuable because criminals can use it to target victims with frauds and scams.

122. As with non-medical identity theft, dealing with the repercussions can be a confusing, time-consuming and costly process, but medical identity theft can also be more dangerous than other forms of identity fraud because it can lead to life-threatening errors in medical records and consequently treatments.[44]

123. The Data Breach was a direct and proximate result of Defendant's failure to: (i)

---

[42] *Id.*

[43] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Oct. 31, 2022).

[44] https://www.experian.com/blogs/ask-experian/how-prevent-medical-identity-theft/ (last accessed Oct. 31, 2022).

properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure as required by various state and federal regulations, industry practices and common law; (ii) establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (iii) protect against reasonably foreseeable threats to the security or integrity of such information.

124. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems.

125. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

126. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had Private information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[45]

127. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial

[45] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at https://bjs.ojp.gov/content/pub/pdf/vit12.pdf (last accessed Oct. 31, 2022).

costs and time to repair the damage to their good name and credit record."[46]

128. What's more, Private Information constitutes a valuable property right, the theft of which is gravely serious.[47] Its value is axiomatic, considering the value of Big Data in corporate America, and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

129. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PII and/or PHI information is stolen and when it is used.

130. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[48]

131. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

132. There is a strong probability that entire batches of stolen information have been

---

[46] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p.2, the GAO (June 2007), available at https://www.gao.gov/assets/gao-07-737.pdf (last accessed Oct. 31, 2022).

[47] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets") (citations omitted).

[48] *Id.*

dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

REPRESENTATIVE PLAINTIFF EXPERIENCE

133. Plaintiff Irene Chabak entrusted her Private Information to Defendant.

134. Specifically, Plaintiff was a patient at Defendant's anesthesia provider practice, Anesthesia Associates of El Paso, Texas.

135. As a condition of receiving Defendant's products and services, Plaintiff disclosed her Private Information.

136. Plaintiff provided her Private Information to Somnia and trusted that the information would be safeguarded according to internal policies and state and federal law.

137. At the time of the Data Breach, Defendant retained Plaintiff's name, address, diagnostic information, and health insurance information.

138. On October 24, 2022, Defendant notified Plaintiff that its computer systems have been accessed and Plaintiff's Private Information had been involved in the Data Breach.

139. Plaintiff is very careful about sharing her sensitive PII and PHI. Plaintiff has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

140. Plaintiff stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

141. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice

of Security Incident, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred.

142. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate her damages by, among other things, monitoring her health care accounts for accuracy.

143. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

144. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

PLAINTIFF'S & CLASS MEMBERS' DAMAGES

145. Plaintiff and Class Members have suffered injury sufficient to confer standing under Article III of the United States Constitution.

146. Plaintiff and Class Members have an "increased risk of identity theft or fraud following the unauthorized disclosure of their data." *McMorris v. Lopez*, 995 F.3d 295, 300-01 (2d Cir. 2021).

147. First, and most importantly, their Private Information has been compromised as the result of the Data Breach.

148. A third party intentionally targeted Defendant's computer system and stole plaintiffs' Private Information stored on that system. *See McMorris v. Lopez,* 995 F.3d 295, 301 (2d Cir. 2021), quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those

consumers' identities.").

149. The type of data at issue here will likely subject Plaintiff and Class Members to a perpetual risk of medical or other identity theft or fraud.

150. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[49]

151. To date, Defendant and/or its affiliate only "encourage [victims] to vigilantly monitor [their] financial statements and credit report." [50]

152. Defendant's Notice to Plaintiff states that Defendant will provide credit monitoring services and other identity theft protection services for only one year.

153. The offer is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

154. Furthermore, Defendant's credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

155. Rather than automatically enrolling Plaintiff and Class Members in credit

---

[49] *See* IdentityTheft.gov by the Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Oct. 31, 2022).

[50] *See* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-649.pdf; *see also* https://elpasoheraldpost.com/notice-of-data-security-incident-anesthesia-associates-of-el-paso-pa/ (patients "should monitor credit reports and financial statements for suspicious activity").

monitoring services upon discovery of the Data Breach, Defendant merely sent instructions offering the services to affected patients with the recommendation that they sign up for the services.

156. Defendant's Notice is also inadequate because it fails to specify exactly what financial and medical information Somnia allowed to be accessed in the Data Breach.

157. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

158. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

159. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

160. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

161. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

162. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion and other illegal schemes based on their PII and PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

163. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

164. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have

recognized the propriety of loss of value damages in related cases.

165. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

166. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

167. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal, medical and financial information is not accessible online and that access to such data is password-protected.

168. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

169. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress and loss of privacy and are at an increased risk of future harm.

170. Moreover, Defendant's delay in identifying and reporting the Data Breach caused additional harm as it is self-evident that early notification can also help limit the liability of a victim in many cases.

171. Indeed, once a data breach has occurred, "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports.

172. And notifying officials can help them catch cybercriminals and warn other

businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[51]

173. Although Defendant experienced a data breach which led to unauthorized exposure of patients' Private Information on or about July 11, 2022 or July 15, 2022, Somnia did not issue any notice until at least two months later, depriving Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

174. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members needlessly increased.

NEW YORK LAW SHOULD APPLY TO PLAINTIFF AND THE CLASS AS WHOLE

175. The State of New York has a significant interest in regulating the conduct of businesses operating within its borders.

176. That is, New York, which seeks to protect the rights and interests of New York and all residents and citizens of the United States against a company headquartered and doing business in New York, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

177. The principal place of business and headquarters of Defendant, located at 450 Mamaroneck Ave, Suite 201 Harrison, New York, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate Defendant's and its affiliates' activities, including major policy, financial and legal decisions.

178. Defendant's actions and corporate decisions surrounding the allegations made herein were made from and in New York.

[51] https://www.consumerreports.org/data-theft/the-data-breach-next-door-a7102554918/ (last accessed Oct. 31, 2022).

179. Defendant's breaches of duty to Plaintiffs and Class Members emanated from New York.

180. Application of New York law to the Class with respect to Plaintiffs' and the Class' claims is neither arbitrary nor fundamentally unfair because New York has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Class.

181. Under New York's choice of law principles, which are applicable to this action, the common law of New York applies to the nationwide common law claims of all Class members. In addition, given New York's significant interest in regulating the conduct of businesses operating within its borders, and that New York has the most significant relationship to Defendant, as it is headquartered in New York and its executives and officers are located and made decisions which led to the allegations of this litigation there, there is no conflict in applying New York law to non-resident consumers such as Plaintiffs and the Class.

CLASS ACTION ALLEGATIONS

182. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

183. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach announced by Defendant on or about October 21, 2022 (the "Class").

184. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

185. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery and before the Court determines whether certification is appropriate. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

186. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Defendant has identified at least 380,104 persons whose Private Information may have been compromised in the Data Breach, and the victims are apparently identifiable within Defendant's records.

187. **Commonality and Predominance**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

b. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

c. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

d. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

e. When specifically Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

h. Whether Defendant's data security systems prior to and during the

Data Breach complied with applicable data security laws and regulations;

i. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

j. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

k. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

l. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

m. Whether Defendant's conduct was negligent;

n. Whether Defendant's conduct was *per se* negligent;

o. Whether Defendant was unjustly enriched;

p. Whether Defendant violated the state consumer protection law asserted herein; and

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

188. Defendant engaged in a common course of conduct giving rise to the legal rights Plaintiff and Class Members seek to enforce, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale in comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

189. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the

Data Breach.

190. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class in that she has no disabling conflicts of interest that would be antagonistic to that of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

191. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources and protects the rights of each Class member.

192. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

193. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

194. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

195. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

196. Finally, all members of the proposed Class are readily ascertainable and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

197. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

198. Defendant obtained Plaintiff's and Class Members' Private Information as a condition of providing services to Plaintiff and Class Members in the State of New York.

199. Defendant's acceptance and maintenance of this information is for its own pecuniary gain and as part of its regular business activities.

200. Plaintiff and the Class Members entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

201. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

202. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their consumers' Private Information involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

203. By assuming the responsibility to collect and to store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information

held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement security protocols and processes by which it could detect a breach of its network servers in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

204. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

205. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

206. Defendant breached its duties (and thus was negligent) by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures and appropriate procedures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its computer system had plans in place to maintain reasonable data security safeguards;

d. Failing to meet the minimum industry standards for preventing cyberattacks and data breaches;

e. Improperly and inadequately safeguarding the Private Information of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach;

f. Failing to heed industry warnings and alerts to provide adequate safeguards to protect consumers' Private Information in the face of increased risk of theft;

g. Allowing unauthorized access to Class Members' Private Information;

h. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Failing to timely and adequately notify Class Members about the existence and scope of the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

207. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

208. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

209. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

210. Plaintiff and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

211. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

212. Defendant had and continues to have a duty to adequately and promptly disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

213. Defendant has admitted that Plaintiff's and Class Members' Private Information was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

214. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

215. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

216. As a result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

217. Additionally, as a direct and proximate result of Defendant's negligence Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

218. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide and continue to provide adequate credit monitoring to all Class Members.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

219. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

220. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of their use of Defendant's services.

221. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized access and disclosure.

222. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

223. When Plaintiff and Class Members provided their PII and PHI to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

224. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

225. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure, including monitoring its computer systems and networks to ensure that it adopted reasonable data security measures.

226. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

227. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

228. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

229. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

230. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide and continue to provide adequate credit monitoring to all Class Members.

COUNT III

UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

231. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

232. Upon information and belief, Defendant funds its data security measures from its general revenue including payments made by or on behalf of Plaintiff and the Class Members.

233. As such, a portion of the payments made by or on behalf of Plaintiff and the Class

Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

234. Plaintiff and Class Members conferred a monetary benefit on Defendant.

235. Specifically, they purchased goods and services from Defendant and/or its agents or contracting partners and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

236. Defendant was aware that any payment for its services from entities that provided consumer information was intended for it on behalf of the consumer as each individual for which Defendant maintained private information was identifiable via the information Defendant collected.

237. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

238. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

239. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed

to implement appropriate data management and security measures that are mandated by industry standards.

240. Defendant failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

241. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

242. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

243. Plaintiff and Class Members have no adequate remedy at law.

244. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the Private Information compromised as a result of the Data Breach, for the remainder of the lives of Plaintiff and Class Members.

245. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

246. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and Class Members the proceeds that it unjustly received from them.

COUNT IV

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff & All Class Members)

247. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

248. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

249. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare, dental, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

250. Defendant's violation of 45 C.F.R. § 164.530(c)(l) and related HIPAA provisions constitutes negligence *per se*.

251. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

252. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

253. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

254. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

255. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

256. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which—as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the same harm as that suffered by Plaintiff and Class Members.

257. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

258. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

259. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered and will continue to suffer injury and damages as alleged herein, and are entitled to compensatory, consequential and punitive damages in an amount to be proven at trial.

COUNT V

VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and All Class Members)

260. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

261. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. promising to maintain the privacy and security of Plaintiffs' protected health information as required by law;

b. failing to maintain adequate computer systems and data security practices to safeguard Private Information;

c. failing to disclose that its computer systems and data security practices were inadequate to safeguard Private Information from theft;

d. continued gathering and storage of Private Information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach; and

e. continued gathering and storage of PII and PHI after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

262. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA, and NY GBL § 349.

263. The foregoing deceptive acts and practices were directed at consumers.

264. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of Plaintiff's and Class Members' Private Information.

265. Defendant's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth are material in that they relate to matters which reasonable persons, including Plaintiff and Class Members, would attach importance to in making their decisions and/or conducting themselves regarding the services received from Defendant.

266. Plaintiff and Class Members are consumers who paid for healthcare services and treatments provided by Defendant, the costs of which necessarily included the amounts Defendant's affiliate providers paid to Defendant for the furnishing of various healthcare-related services.

267. Defendant's acts, practices and omissions were done in the course of Defendant's business of furnishing healthcare-related services to consumers in the State of New York.

268. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and Class Members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect

the Private Information in its continued possession; (vi) future costs in terms of time, effort and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

269. Also as a direct result of Defendant's violation of GBL §349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) immediately provide and continue to provide adequate credit monitoring to all Class Members.

270. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

271. Defendant knew or should have known that its network systems and data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

272. Plaintiff and Class Members were injured because: (i) they would not have paid for services provided by the Defendant had they known the true nature and character of Defendant's data security practices; (ii) Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and (iii) Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopts reasonable data security measures.

273. As a result, Plaintiffs and the Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT VI

VIOLATIONS OF NEW YORK'S INFORMATION SECURITY BREACH AND NOTIFICATION ACT (N.Y. Gen. Bus. Law § 899-aa, *et seq*.) (On Behalf of Plaintiff and All Class Members)

274. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

275. The acts and practices alleged herein occurred in trade or commerce in the state of New York.

276. The Data Breach, which compromised the Private Information of New York citizens, constitutes a "breach of security," as that term is defined by NY Gen. Stat. §899-aa.

277. In the manner described herein, Defendant unreasonably delayed the disclosure of the "breach of security" of Private Information within the meaning of NY Gen. Stat. § 899-aa.

278. Pursuant to NY Gen. Stat. § 899-aa the Defendant's failure to disclose the Data Breach following its discovery to each New York resident whose Private Information was, or was reasonably believed to have been, accessed by an unauthorized person through the Data Breach, constitutes an unfair trade practice pursuant to NY Gen. Stat. § 899-aa.

COUNT VII

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT (On Behalf of Plaintiff and All Class Members)

279. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

280. Somnia entered into a contract to provide services to its customers, including Plaintiff and Class Members and/or their respective medical providers.

281. These contracts were made expressly for the benefit of Plaintiff and the Class Members, as it was their confidential medical information that Somnia agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

282. Somnia knew that if it were to breach these contracts with its customers, the customers' patients, including Plaintiff and the Class Members, would be harmed by, among other harms, fraudulent transactions.

283. Somnia breached its contracts with its customers affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

284. As foreseen, Plaintiffs and the Class Members were harmed by Defendant's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their Private Information.

285. Accordingly, Plaintiffs and the Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Irene Chabak respectfully prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant' wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and Class Members;

f) For an award of actual damages, compensatory damages, statutory damages and statutory penalties in an amount to be determined and as allowable by law;

g) For an award of punitive damages as allowable by law;

h) For an award of attorneys' fees and costs and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this Honorable Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff respectfully demands a trial by jury on all claims so triable.

Dated: October 31, 2022

Respectfully submitted,

WEITZ & LUXENBERG, PC

/s/ James Bilsborrow

James Bilsborrow (JB8204)
700 Broadway
New York, NY 10003
(212) 558-5500

Counsel for Plaintiff and the Putative Class